1. 依據

* 美國聯邦法規 10 CFR 73.54
* 美國核能管制委員會 2010 年發布的法規指引 RG 5.71
* 行政院科技顧問組於「2010 資通安全政策白皮書」

1. 目的

* 根據美國聯邦法規10 CFR 73.54要求，核電廠必須建立、實施、及維護資通安全計畫，以保護核電廠安全、保安、對安全重要及緊急應變等相關之關鍵數位資產免於遭受資通攻擊。

1. 適用範圍

* 資通安全計畫針對具備下列功能之數位計算機、通訊系統與網路，抵擋資通安全攻擊：
  + 安全相關及對安全具重要性之功能
  + 保安功能
  + 應變整備功能，包含單位離線通訊
  + 對安全、保安、或應變整備功能產生不利影響的支援系統與裝備

1. 資通安全計畫

* 資通安全計畫將說明核電廠如何適當地保護與安全、保安、及應變整備功能(safety, security, and emergency preparedness : SSEP)相關之數位計算機、通訊系統、及網路，確保抵擋資通攻擊。
* 核電廠必須經由原能會核准之實體保安計畫、訓練品質計畫、保全員意外應變計畫、資通安全計畫，以確保和電廠運作安全。資通安全計畫為核電廠實體保安計畫一部分。

1. 資通安全實施程序
   1. 組成資通安全小組

* 核電廠應明訂關鍵數位資產資通安全規劃、評估和授權政策，定義目的、範圍、角色、責任和管理者角色與責任，並協調相關單位部門推動關鍵數位資產資通安全計畫之管控措施。
* 核電廠應建立及維持一個資通安全小組，納編資通安全、通訊系統、系統管理、電腦網路、數位儀控、核電廠設施運作與規範…等知識專才組成資通安全小組
* 資通安全小組(CST)的角色與責任
  + 執行或監督資通安全管理程序
  + 記錄安全管理過程中重要觀察、分析結果與發現
  + 評估資通安全威脅、潛在弱點與攻擊結果
  + 評估資通安全管控、防護政策、及減緩攻擊方法的效益
  + 資通安全教育訓練與資安事件認知
  + 蒐集數位資產現場檢查與資通安全管控過程資訊
  + 發現與執行新的管控措施
  + 紀錄未實施資通安全管控措施的替代方法
  + 確保所有評估文件之保存
  1. 辨識關鍵數位資產
* 辨識影響核電廠安全、保安、及應變整備功能之數位電腦、通訊系統、及網路能。
* 資通安全小組藉由核電廠系統、裝備、與網路等分析，辨識哪些系統被危及、過度使用、或失效，將影響核電廠安全、保安、及應變整備功能，以發現關鍵系統。並對影響核電廠安全、保安、及應變整備功能相關的支援系統或裝備，根據相依性及路徑分析決定哪些系統或裝備為關鍵系統。
* 資通安全小組辨識關鍵系統的正常功能扮演直接、支援、或間接角色的關鍵數位資產，並針對每一個關鍵數位資產進行審查及驗證。
  1. 建立深度防禦策略
* 持照者應依據一個深度防護策略(defense-in-depth strategy)用以設計資通安全程序，以確保資通攻擊事件之偵測、防範、反應、減緩、及復原能力。深度防護策略應包括安全防護架構與安全管控措施
* 深度防護策略代表多層次的關鍵數位資產保護，可以由資料通訊、資訊傳遞路徑、及實體區訪護等方面來定義不同階層。
  1. 資通安全管控措施
* 存取控制
* 稽核與責任
* 系統與通訊防護
* 識別與鑑別
* 系統強化
* 資訊媒體防護
* 個人安全
* 系統與資訊網整防護
* 維護
* 實體與環境防護
* 安全評估與風險管理
  1. 資安事件通報流程
* 緊急應變計畫
* 資安事件反應
* 資安事件通報

1. 整合資通安全至實體保安計畫

* 建立一個統一的安全組織，整合資通與實體安全，說明實體與資通安全之相互依存關係。
* 發展政策與程序統一管理及整合實體與資通安全管控措施。
* 協調籌獲實體或通資安全服務、訓練、裝置與設備。
* 協調相依的實體與資通安全活動，及實體與資通安全人員的訓練。

1. 資通安全計畫維護

* **持續監測與評估**
* **弱點評估與掃描**
* **變動管制**

1. 文件與記錄保留處理

* 持照者建立必要的評量與管理程序，以確保發展、審查、核准、發表、使用、修正足夠影響通資安全項目與活動的紀錄。
* 持照者須保存與支援符合 10 CFR 73.54 與 10 CFR 73.55 要求的技術文件
* 保存的紀錄包括可用於紀錄、分析網絡與關鍵數位資產(CDA)事件的所有的數位記錄、紀錄檔案、機和檔案、及非數位紀錄。這些將存取歷史紀錄為文件及探索資通攻擊的來源或影響關鍵數位資產(CDA)或SSEP功能或包含兩者的安全相關的事件。
* 除非核管單位另有規定，持照者應將這些記錄至少要保留三年，直到被取代更，。